536,817

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051581 A1

(51) International Patent Classification[7]: G07C 9/00, B60R 25/00

(21) International Application Number: PCT/IB2003/005378

(22) International Filing Date: 24 November 2003 (24.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 55 880.9 29 November 2002 (29.11.2002) DE

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NOWOTTNICK, Jürgen** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **MEYER, Michael**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

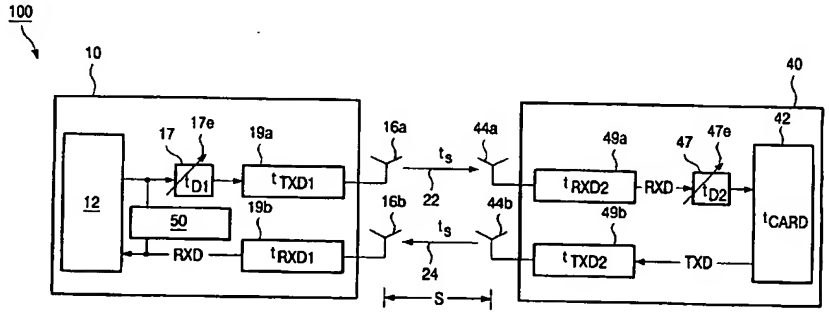
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ELECTRONIC COMMUNICATION SYSTEM AND METHOD OF DETECTING A RELAY ATTACK THEREON



(57) Abstract: In the case of an electronic communication system (100) having; a) at least one base station (10) having at least one antenna unit (16: 16a, 16b), in particular in coil form, which base station (10) is arranged in particular on or in an object to be secured against unauthorized use and/or against unauthorized access, such as on or in, say, a means of transport or on or in an access system, and, b) at least one transponder station (40), in particular in data-carrier form, having at least one antenna unit (44: 44a, 44b), in particular in coil form, which transponder station (40), c) may in particular be carried with him by an authorized user and/or, d) is designed to exchange data signals (22, 24) with the base station (10), in which case, by means of the data signals (22, 24), e) the authorization for use and/or access can be determined and/or, f) the base station (10) can be controlled accordingly,and in the case of a method of detecting and/or guarding against at least one, in particular external, attack, and preferably at least one relay attack, on an electronic communication system (100) of this kind, to enable the electronic communication system (100) and the method to be further developed in such a way that the attack is at least made substantially more difficult and if possible is fully guarded against and prevented, it is proposed that, g) there be arranged in the base station (10) at least one first delay element (17) for setting a defined, and in particular substantially constant, signal transit time (t_1) within the base station (10) and/or, h) there be arranged in the transponder station (40) at least one second delay element (47) for setting a defined, and in particular substantially constant, signal transit time (t_2) within the transponder station (40).

WO 2004/051581 A1

Electronic communication system and method of detecting a relay attack thereon

The present invention relates in general to the technical field of security and/or access systems, and in particular to that of so-called P[assive K[eyless] E[ntry] systems, such as are used, for example, in the area of means of transport and in this case above all in the area of access systems for motor vehicles.

Specifically, the present invention relates to an electronic communication system as detailed in the preamble to the main claim, and to a method of detecting and/or guarding against at least one attack, and particularly an external attack and preferably at least one relay attack, on at least one electronic communication system as detailed in the preamble to the main claim.

To produce electronic communication systems, and particularly P[assive K[eyless] E[ntry] systems, of the kind specified above that have amongst other things a conventional passive transponder system, use is conventionally made of various configurations. One possible configuration is shown in Figs. 1A and 1B of the drawings, the example used being that of a P[assive K[eyless] E[ntry] system for a motor vehicle:

Between a so-called base station 10, that is fitted with an antenna unit 16 in the form of a coil, and a transponder station 40, a communication sequence in the form of a data exchange takes place:

In detail there are, as signal-transmission links between the base station 10 and the transponder station 40, a so-called up-link frame 22 that is formed, for example, by at least one inductively coupled L[ow]F[requency] channel and over which signals are transmitted from the base station 10 to the transponder station 40, and a so-called down-link frame 24 that is formed, for example, by at least one U[ltra]H[igh]F[requency] channel and over which signals are transmitted from the transponder station 40 to the base station 10. As an alternative to this, both the up-link frame 22 and the down-link frame 24 may each be formed by at least one L[ow]F[requency] channel or, as an alternative to this in turn, both the up-link frame 22 and the down-link frame 24 may each be formed by at least one U[ltra]H[igh]F[requency] channel.

After, for example, a door handle of the motor vehicle or a pushbutton on a door of the vehicle has been operated, the base station 10, which is spatially and functionally

associated with the motor vehicle, begins to generate a signal that is referred to as a "challenge" and that is transmitted to the transponder station 40 via the up-link frame 22. A circuit arrangement 42 in the transponder station 40, which is preferably equipped with at least one microprocessor, then calculates from the challenge, using a cryptographic algorithm and a secret key, a signal sequence that is referred to as a "response". This response signal is then transmitted from the transponder station 40 to the base station 10 via the down-link frame 24.

The base station 10 then compares the response, using an identical crypto-algorithm and an identical secret key. If identity is found, the base station 10 causes the door lock of the motor vehicle to open, i.e. only if, generally by using cryptographic methods, the authentication process recognizes the transponder station 40 as valid is, in the embodiment given as an example, the door lock of the motor vehicle opened.

If, however, this circuit arrangement is operated in the form shown in Figs. 1A and 1B without any other added technical provisions, there is a danger that an external attacker, who is attempting to open the door of the vehicle without being authorized to do so, may carry out a so-called "relay attack", as described below, using relatively little in the way of technical resources.

Shown diagrammatically in Figs. 2A and 2B is an arrangement for carrying out a relay attack of this kind. For this purpose, there is introduced into the configuration shown in Figs. 1A and 1B an "attacker kit" in the form of an additional transmission link 30 that comprises a first relay 32 in the form of an emulator for the transponder station, a second relay 36 in the form of an emulator for the base station, and a communications link 35 between the first relay 32 and the second relay 36.

In this connection, the communications link 35 between the first relay 32 and the second relay 36 may take the form of at least one bi-directional transmission channel of any desired type that allows there to be a random distance between the first relay 32 and the second relay 36.

To allow inductive coupling to the antenna unit 16 of the base station 10, the first relay 32 in the form of the transponder station emulator is fitted with an associated antenna unit 34 in the form of a coil; similarly, the second relay 36 in the form of the base station emulator is fitted with an associated antenna unit 38 in the form of a coil for inductive coupling to an antenna unit 44 in coil form of the transponder station 40.

One attacker then takes up position in the immediate vicinity of the motor vehicle with the first relay 32. A second attacker positions himself sufficiently close to the

valid transponder station 40 with the second relay 36. Triggered by, for example, the operation of a door handle of the motor vehicle or of a pushbutton on a door of the motor vehicle, the base station 10 in the motor vehicle transmits its challenge to the first relay 32 by means of the original, i.e. unemulated, up-link frame 22.

From this first relay 32, the challenge is passed on via the above-mentioned communications link 35 to the second relay 36. The second relay 36 emulates the up-link 22 and in this way passes on the challenge to the valid transponder station 40 by means of the antenna unit 38 in coil form. Once the response has been calculated in the valid transponder station 40, this transponder station 40 responds to the second relay 36 by transmitting this response by means of the original, i.e. non-emulated down-link frame 24.

From this second relay 36, the response is passed on via the above-mentioned communications link 35 to the first relay 32. The first relay 32 emulates the down-link frame 24 and in this way passes on the response to the valid base station 10 in the motor vehicle by means of the antenna unit 34 in coil form.

Because the response was produced by the authentic transponder station 40 on the basis of the authentic challenge from the base station 10 using the correct crypto-algorithm and the correct key, the response is recognized as valid and the door of the motor vehicle opens, even though the authorized and rightful user does not want this.

In view of the fact that more stringent demands are being made nowadays on the operation and security of certain components, precisely in, for example, the area of automobiles and the area of access, the configuration shown in Figs. 1A and 1B, which can be sabotaged by the measures shown in Figs. 2A and 2B, appears not to be sufficiently secure.

Accordingly, certain proposals for detecting and guarding against relay attacks of this kind have already been made in the past. In printed publication EP 1 136 955 A2 for example, there is disclosed an arrangement for an access-safeguarding system (a P[assive K[eyless] E[ntry] system) by means of which the relative orientation of the base station 10 and the transponder station 40 to one another can be calculated.

Under another proposal, to allow such relay attacks to be detected and guarded against, the time between the challenge and the response is determined to enable an additional delay due to the delays caused by the electronics of the relays and to the additional transit time of the signals between the relay stations to be detected in this way (the transit-time measurement method).

However, it is virtually impossible for a relay attack to be detected by the signal transit-time measurement method in a current transponder system having a carrier frequency of 125 kilohertz, because the stringent requirements for accuracy in the measurement of time can hardly be met in practice, the main reasons for which are tolerances in the filters used and temperature problems.

So, to enable a relay attack to be safely and reliably detected by transit-time measurement, very stringent demands have to be made on the accuracy with which time is measured. Shown in Fig. 3 in schematic form is the principle of a measurement of signal transit-time of this kind, for detecting a relay attack as shown in Figs. 2A and 2B, such as would be used in the case of the prior art embodiment shown in Figs. 1A and 1B. The total signal transit-time works out as follows in this case:

$$t_{total} = t_{TXD1} + t_s + t_{RXD2} + t_{CARD} + t_{TXD2} + t_s + t_{RXD1}$$

A criterion for the occurrence of a relay attack is therefore that, due to the additional relay link, the distance s between the base station 10 and the transponder station 40 exceeds a given maximum permitted distance s_{max}. To allow a relay attack to be detected, this distance s, which can be calculated from the transit time t_s of the signals 22, 24 and the known speed of propagation of the signals 22, 24 using the formula $s = v_s \cdot t_s$, has to be determined as accurately as possible.

However, it has to be remembered that in the case of a signal transit-time measurement as in Fig. 3, the additional delays t_{TXD1}, t_{RXD2}, t_{CARD}, t_{TXD2} and t_{RXD1} are added to the signal transit time t_s that is wanted. For the distance s between the base station 10 and the transponder station 40 to be accurately determined, and hence too for a sufficiently short maximum permitted distance s_{max} (with no great safety reserve) to be selected, these additional components of the signal transit time need to be known, or need to be determined with sufficient accuracy.

Another thing that needs to be borne in mind in this case is that in a practical system to be produced in large numbers at low cost, considerable tolerances Δt_{TXD1}, Δt_{TXD2}, Δt_{RXD1} and Δt_{RXD2} can be expected on the signal transit times due to the electronics of the base station 10 and/or of the transponder station 40. These tolerances are due to the effects of ageing, to scatter among the components used and to the effects of temperature. Unless additional steps are taken, these tolerances too have to be allowed for when determining the threshold value s_{max}.

On the basis of the disadvantages and deficiencies described above and with due acknowledgement of the prior art outlined, it is an object of the present invention to further develop an electronic communication system of the kind described at the beginning, and a method of detecting and/or guarding against at least one external attack, and preferably at least one relay attack, on at least one electronic communication system of the kind described at the beginning, in such a way that the attack is at least made considerably more difficult and if possible is completely guarded against and prevented.

This object is achieved by an electronic communication system having the features specified in claim 1 and by a method having the features specified in claim 7. Advantageous embodiments and useful refinements of the present invention are characterized in the respective sets of dependent claims.

Under the teaching of the present invention

- there is arranged in the base station at least one first adjustable delay element for setting a defined, and in particular substantially constant, signal transit time t_1 within the base station and/or
- there is arranged in the transponder station at least one second adjustable delay element for setting a defined, and in particular substantially constant, signal transit time t_2 within the transponder station.

An additional, adjustable signal propagation delay is thus introduced, in accordance with the invention, into the transmission chain.

By means of the first adjustable delay element and by means of the second adjustable delay element, the signal transit time t_1 within the base station and the signal transit time t_2 with the transponder station can be respectively set, which means that the attack is detected if the sum of the signal transit time t_1 within the base station, the signal transit time t_2 within the transponder station, and twice the signal transit time t_s of the data signals between the base station and the transponder station exceeds a defined threshold value $t_{s,\,max}$.

Hence, the basic idea behind the present invention is to compensate for the signal transit times of the transmitting and receiving units of P[assive K[eyless] E[ntry] systems, suitable technical steps being taken (= arrangement of at least one first adjustable delay element for setting a defined, and in particular substantially constant, signal transit time t_1 within the base station and/or arrangement of at least one second adjustable delay element for setting a defined, and in particular substantially constant, signal transit time t_2 within the transponder station) to ensure as constant as possible a signal propagation delay for the

transmitting and receiving sub-assemblies both at the base station end, e.g. on or in the vehicle to be secured, and at the transponder end, on or in the PKE data carrier (the PKE card).

By suitable regulation and setting of the particular delays t_{D1} and t_{D2} within the base station and transponder station respectively by means of the respective additional delay elements, improved conditions are obtained for detecting and/or guarding against relay attacks, as shown by the following equations:

$t_1 = t_{RXD1} + t_{D1} + t_{TXD1}$ = substantially constant,

$t_2 = t_{RXD2} + t_{D2} + t_{CARD} + t_{TXD2}$ = substantially constant.

A relay attack is therefore taking place if the following threshold value condition is met:

$t_{s,max} < t_1 + t_2 + 2\,t_s = t_{RXD1} + t_{D1} + t_{TXD1} + t_{RXD2} + t_{D2} + t_{CARD} + t_{TXD2} + 2\,t_s$.

In a practical implementation, a comparison may therefore advantageously be made with a fixed threshold $t_{s,max}$, once the latter has been defined, in which case allowance will advantageously have been made for the dependences of the signal transit times on the system tolerances Dt_{TXD1}, Dt_{TXD2}, Dt_{RXD1} and Dt_{RXD2}.

In a particularly inventive refinement of the present electronic communication system and of the method of detecting a relay attack thereon, provision may be made for optional temperature measurement, by means of which it is possible, by using the additional delay elements, to produce ensuing compensation for the temperature dependence with the aim of obtaining total delays t_1 within the base station and t_2 with the transponder station which are each constant and, in particular, non-temperature-dependent.

The (regulating) algorithm for implementing the method according to the present invention may preferably be executed even during a communication between the base station and transponder station, to prevent an external attack on the regulating algorithm by detection of the attacking relays. In this case, the relays have to pass on the data if the protocol is not to be injured.

In an advantageous embodiment of the present invention, the regulating algorithm for producing the signal transit times t1 and t2 may be executed by any desired method, such as, for example, the counting method or the successive approximation method.

The delay element, which is preferably multistage and preferably switchable, may usefully comprise suitable components of any desired kinds such as, say,

- at least one digital gate subject to a known signal transit time and/or
- at least one filter and/or

- at least one clocked shift register.

The man skilled in the art of communications electronics, such as, for example, an electrical engineer having detailed knowledge in the field of security systems, will be particularly appreciative of the fact that the present invention assists in the production of a P[assive K[eyless] E[ntry] system that is highly resistant to external attack, i.e. by an exact measurement of time it makes so-called "relay attack" very much more difficult. In line with this, it becomes possible for an additional exact measurement of time for detecting a relay attack with increased reliability to be implemented in a manner suitable for practical application.

For the practical implementation of the measurement of time, a comparison of the total signal transit time measured may advantageously be made, with great accuracy, with a fixed threshold $t_{s,max}$ subject to tight tolerances, in which case inexpensive modes of implementation that are possible make the electronic communication system and the associated method highly attractive for use in mass production.

The present invention, which extends both to at least one base station of the kind described above and to at least one transponder station of the kind described above, may advantageously also be used in systems that are widely employed in the field of so-called "immobilizer" systems for means of transport and particularly motor vehicles.

Another area of application for the present invention is in the field of building security, because the electronic communication system, with its base station and also with its transponder station, is also superbly well suited to the production of secure access systems based on transponders, and particularly on data carriers such as, say, chip cards or P[assive K[eyless] E[ntry] cards.

Hence, the base station may be arranged on or in an object or building that is to be secured against unauthorized use and/or against unauthorized access, such as on or in a means of transport, say, or on or on an access system.

As has already been discussed above, there are various possible ways in which the teaching of the present invention may advantageously be embodied and refined. These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

In the drawings:

Fig. 1A is a schematic view showing the principle of communication, based on inductive coupling, between a base station and an associated transponder station as in a prior art embodiment.

Fig, 1B is the equivalent electrical circuit diagram of the principle of communication shown in Fig. 1A.

Fig. 2A is a schematic representation of a so-called "relay attack" on the prior art embodiment shown in Figs. 1A and 1B.

Fig. 2B is the equivalent electrical circuit diagram of the relay attack shown in Fig. 2A.

Fig. 3 is a schematic representation of the principle on which signal transit time is measured to allow the relay attack shown in Figs. 2A and 2B to be detected, in the case of the prior art embodiment shown in Figs. 1A and 1B.

Fig. 4 is a schematic representation of the principle of measurement according to the present invention for detecting the relay attack shown in Figs. 2A and 2B, which principle is based on the production of constant signal transit times, in an embodiment according to the present invention, and

Fig. 5 is a schematic representation of the measures according to the present invention for regulating the delay to signal propagation within the base station and/or within the transponder station to constant signal transit time values as in Fig. 4.

Arrangement, elements or features that are the same or similar in Figs. 1A to 5 are given the same reference numerals.

As is shown in Fig. 4 by an embodiment, what is implemented by means of the present invention is an electronic communication system 100 that has, amongst other things, a transponder system (= transponder station 40 in the form of a data carrier, namely a P[assive K[eyless] E[ntry] card), which in turn is part of a system for opening and closing the door locks of a motor vehicle.

The PKE card 40 has a receiver unit 49a having a signal transit time t_{RXD2}, the receiver unit 49a being connected to an antenna unit 44a and being used to receive data signals 22 from a base station 10. The PKE card 40 also has a transmitter unit 49b having a signal transit time t_{TXD2}, the transmitter unit 49b being connected to an antenna unit 44b and being used to transmit data signals 24 to the base station 10. Connected downstream of the receiver unit 49a and upstream of the transmitter unit 49b is a control unit 42 (--> signal

transit time t_{CARD}) in the form of a microcontroller unit that is provided to control the PKE card 40.

A base station 10 that is also shown in Fig. 4 has a receiver unit 19b having a signal transit time t_{RXD1}, the receiver unit 19b being connected to an antenna unit 16b and being used to receive data signals 24 from a PKE card 40. The base station 10 also has a transmitter unit 19a having a signal transit time t_{TXD1}, the transmitter unit 19a being connected to an antenna unit 16a and being used to transmit the above-mentioned data signals 22 to the PKE card 40. Connected downstream of the receiver unit 19b and upstream of the transmitter unit 19a is a control unit 12 in the form of a microcontroller unit that is provided to control the base station 10.

When the PKE card 40 is in the active state (see Fig. 4), a communication sequence intended for authentication purposes takes place in the form of an exchange of data between the base station 10 and the PKE card 40, for which purpose data signals 22, 24 are exchanged between the base station 10 and the transponder station 40; by means of these data signals 22, 24, not only can authorization to use and/or access the motor vehicle be determined but the base station 10 can also be controlled in the appropriate way. In the case of P[assive K[eyless] E[ntry] which is being described here, the power supply may preferably be supplied by at least one battery unit.

In detail, what exist as signal transmission links between the base station 10 and the PKE card 40 are a so-called "up-link frame" 22 that is formed by, for example, at least one inductively coupled L[ow]F[requency] channel and via which signals are transmitted from the base station 10 to the PKE card 40, and a so-called "down-link frame" 24 that is formed by, for example, at least one U[ltra]H[igh]F[requency] channel and via which signals are transmitted from the PKE card 40 to the base station 10.

However, it is also within the scope of the present invention for both the up-link frame 22 and the down-link frame 24 each to be formed by at least one L[ow]F[requency] channel in the embodiment shown in Figs. 4 and 5. As an alternative to this, it is in turn also possible for both the up-link frame 22 and the down-link frame 24 each to be formed by at least one U[ltra]H[igh]F[requency] channel.

Once the door lock, for example, of the motor vehicle has been operated, the base station 10 that is functionally and spatially associated with the motor vehicle begins to generate a signal referred to as a "challenge", which is transmitted to the PKE card 40 via the up-link frame 22. An electronic circuit arrangement in the PKE card 40 that is preferably arranged to have at least one microprocessor then calculates from the challenge, using a

cryptographic algorithm and a secret key, a signal sequence that is referred to as a "response". This response signal is then transmitted from the PKE card 40 via the down-link frame 24 to the base station 10.

The base station 10 then compares the response, using an identical crypto-algorithm and an identical secret key; if identity is found, the base station 10 then causes the motor vehicle's door lock to be opened, or in other words, only if the authentication recognizes the PKE card 40 as valid, generally by the use of cryptographic methods, is the door lock of the motor vehicle opened in the embodiment cited.

In order now to provide resistance to relay attacks of the kind described by reference to Figs. 2A and 2B, there is arranged in the base station 10 a first delay element 17 that is connected downstream of the control unit 12 and upstream of the transmitter unit 19a and that is used to set a defined, substantially constant, signal transit time t_1 within the base station 10. Similarly, there is arranged in the PKE card 40 a second delay element 47 that is connected downstream of the receiver unit 49a and upstream of the control unit 42 and that is used to set a defined, substantially constant, signal transit time t_2 within the PKE card 40.

An external relay attack is now detected if the sum of

- the signal transit time t_1 within the base station 10,
- the signal transit time t_2 within the PKE card 40, and
- twice (<--> "out" signal 22 and "back" signal 24) the signal transit time t_s between the base station 10 and the PKE card 40

exceeds a defined threshold value $t_{s,max}$, that is to say if the threshold value condition

$$t_{s,max} < t_1 + t_2 + 2t_s \quad \text{or}$$

$$t_{s,max} < t_{RXD1} + t_{D1} + t_{TXD1} + t_{RXD2} + t_{D2} + t_{CARD} + 2t_s$$

is met, where

- the signal transit time t_1 within the base station 10 is composed, in essence, of
  - -- the signal transit time t_{RXD1} within the receiver unit 19b
  - -- the delay in signal transit time t_{D1} caused by the first delay element 17, and
  - -- the signal transit time t_{TXD1} within the transmitter unit 19a

and

- the signal transit time t_2 within the PKE card 40 is composed, in essence, of
  - -- the signal transit time t_{RXD2} within the receiver unit 49a
  - -- the delay in signal transit time t_{D1} caused by the second delay element 47
  - -- the signal transit time t_{CARD} with the control unit 42, and
  - -- the signal transit time t_{TXD2} within the transmitter unit 49a

and t_s is once the signal transit between the base station 10 and the PKE card 40 and $2t_s$ is therefore twice this signal transit time.

To then enable this basic idea of the present invention to be implemented, namely the use of a constant signal propagation delay t_1 (--> base station 10) or t_2 (--> PKE card 40), that is defined once, for the electronic sub-assemblies for transmitting and receiving the data exchanged between the motor vehicle (--> base station 10) and the P[assive K[eyless] E[ntry] card 40, both the first delay element 17 within the base station 10 and the second delay element 47 within the PKE card 40 (see reference numerals 17e and 47e respectively) are arranged to be adjustable in four stages (see reference numerals 17a, 17b, 17y, 17z and 47a, 47b, 47y, 47z respectively) and switchable (see reference numerals 17s and 47s respectively), in the form of, for example

- at least one digital gate subject to a known signal transit time and/or
- at least one filter and/or
- at least one clocked shift register.

To regulate the delay times t_1 and t_2 applicable to signal propagation to constant values, there are various technical implementations that are obvious possibilities. In what follows, a simple and inexpensive implementation employing regulation of the transit time will be described by reference to the detailed representation in Fig. 5, first by taking the base station 10 as an example:

A pulse to be transmitted from the base station 10 to the PKE card 40 is conveyed to the multistage (see reference numerals 17a, 17b, 17y) and switchable (see reference numeral 17s) first delay element 17. The delayed pulse is then fed to the transmitter (= transmitter unit 19a of the base station 10) and is received directly, i.e. with no relevant additional delay in signal propagation, by the receiver (= receiver unit 19b of the base station 10). At the same time, the pulse is also fed through the entire delay line, i.e. through all four stages 17a, 17b, 17y, 17z of the first delay element 17 (-> delay time t_1).

A decision-maker (= first decision-making unit 18 of the base station 10) that is connected downstream of the fourth and last stage 17z of the delay element 17 and that is connected to the receiver unit 19b signals to the control unit 12 which of the two pulses ("delayed pulse" or "pulse fed through the entire delay line") arrives at the first decision-making unit 18 first.

In conjunction with a regulating algorithm that is implemented in the control unit 12, the switchable delay element 17 is set or corrected in such a way that the two pulses arrive as near simultaneously as possible; in this event, where the delayed pulse and the pulse

that has been fed through the entire delay line arrive substantially simultaneously, the desired constant total delay t_1 in signal propagation is produced.

In what follows, an implementation employing regulation of the transit time will be described, also by reference to the detailed representation in Fig. 5, by taking the PKE card 40 as an example, which will show that the method described above for easily and inexpensively regulating signal transit times can be used in a similar or analogous fashion for compensating for the signal transit times in the PKE card 40.

A pulse transmitted from the base station 10 to the PKE card 40 is conveyed to the multistage (see reference numerals 47a, 47b, 47y) and switchable (see reference numeral 47s) second delay element 47. At the same time, the pulse is also fed through the entire delay line, i.e. through all four stages 47a, 47b, 47y, 47z of the second delay element 47 (-> delay time t_2).

A decision-maker (= second decision-making unit 48 of the PKE card 40) that is connected downstream of the fourth and last stage 47z of the delay element 47 and that is connected to the transmitter unit 49b signals to the control unit 42 which of the two pulses ("delayed pulse" or "pulse fed through the entire delay line") arrives at the second decision-making unit 48 first.

In conjunction with a regulating algorithm that is implemented in the control unit 42, the switchable delay element 47 is set or corrected in such a way that the two pulses arrive as near simultaneously as possible; in this event, where the delayed pulse and the pulse that has been fed through the entire delay line arrive substantially simultaneously, the desired constant total delay t_2 in signal propagation is produced.

So, what can be said as a result is that compensation for the tolerances on the signal transit times of transmitter and receiver units is obtained by means of the electronic communication system 100 shown in Figs. 4 and 5 and by means of the method associated with this communication system 100, which compensation may advantageously be employed in P[assive K[eyless] E[ntry] systems or in similar configurations. In such systems, the present invention implements a form of transit time measurement by means of which a potential external attack in the form of a so-called relay attack can be detected and/or guarded against.

In this case, both the electronic communication system 100 described and the method described constitute a flexible, cost-efficient, novel and inventive extension of signal transit time measurements which were possible in the prior art, to enable these latter to be

used even under practical conditions. The accuracy and reliability of the principle of time measurement (see the time measuring unit 50 in Fig. 4) are increased in this case.

In this connection, typical incidental conditions that made it difficult for signal transit time measurement to be used in the past are overcome in accordance with the invention, such as, say

- scatters in the signal transit times within the transmitter and receiver due to tolerances on the components
- changes in the signal transit times within the transmitter and receiver due to the effects of temperature and to ageing, and/or
- the pressure of costs when used in mass production.

The present invention may with advantage be used in P[assive K[eyless] E[ntry] systems, which are being used to an increasing degree in the field of access systems for motor vehicles. What is more, the electronic communication system 100 described and the method described are also suitable for producing secure access systems based on chip cards 40 in the field of building security, in which case the arrangement described that is shown in Figs. 4 and 5 may also be used in a similar way to guard against relay attacks on access/entry systems.

LIST OF REFERENCE NUMERALS

100	Electronic communication system
10	Base station
11	First resistor of base station 10
12	Control unit, in particular microcontroller unit, of base station 10
13	Capacitive unit of base station 10
14	Analog interface of base station 10
15	Second resistor of base station 10
16	Antenna unit of base station 10
16a	Antenna unit of base station 10 associated with transmitter unit 19a
16b	Antenna unit of base station 10 associated with receiver unit 19b
17	First delay element of base station 10
17a	First stage of first delay element 17
17b	Second stage of first delay element 17
17e	Setting facility of first delay element 17
17s	Switching facility of first delay element 17
17y	Stage before last of first delay element 17
17z	Last stage of first delay element 17
18	First decision-making unit of base station 10
19a	Transmitter unit of base station 10
19b	Receiver unit of base station 10
22	Up-link frame
23	Up-link frame emulation
24	Down-link frame
25	Down-link frame emulation
30	Additional transmission link
32	First relay forming an emulator for the transponder station 40
34	Antenna unit of first relay 32
35	Communications link between first relay 32 and second relay 36
36	Second relay forming an emulator for the base station 10
38	Antenna unit of second relay 36
40	Transponder station, in particular a data carrier and specifically a P[assive K[eyless] E[ntry] card

42	Circuit arrangement or control unit, in particular microcontroller unit, of transponder station 40
44	Antenna unit of transponder station 40
44a	Antenna unit of transponder station 40 associated with receiver unit 49a
44b	Antenna unit of transponder station 40 associated with transmitter unit 49b
47	Second delay element of transponder station 40
47a	First stage of second delay element 47
47b	Second stage of second delay element 47
47e	Setting facility of second delay element 47
47s	Switching facility of second delay element 47
47y	Stage before last of second delay element 47
47z	Last stage of second delay element 47
48	Second decision-making unit of transponder station 40
49a	Receiver unit of base station 40
49b	Transmitter unit of base station 40
50	Time measurement facility
s	Distance between base station 10 and transponder station 40
t_1	Signal transit time within base station 10
t_2	Signal transit time with transponder station 40
t_{CARD}	Signal transit time in control unit 42 of transponder station 40
t_{D1}	Delay in transit time within first delay element 17 of base station 10
t_{D2}	Delay in transit time within second delay element 47 of transponder station 40
t_{RXD1}	Signal transit time in receiver unit 19b of base station 10
Δt_{RXD1}	Tolerance on signal transit time in receiver unit 19b of base station 10
t_{RXD2}	Signal transit time in receiver unit 49a of transponder station 40
Δt_{RXD2}	Tolerance on signal transit time in receiver unit 49a of transponder station 40
t_s	Signal transit time between base station 10 and transponder station 40
t_{total}	Total signal transit time in the electronic communication system 100
t_{TXD1}	Signal transit time in transmitter unit 19a of base station 10
Δt_{TXD1}	Tolerance on signal transit time in transmitter unit 19a of base station 10
t_{TXD2}	Signal transit time in transmitter unit 49b of transponder station 40
Δt_{TXD2}	Tolerance on signal transit time in transmitter unit 49b of transponder station 40

V_s Speed of signal propagation between base station 10 and transponder station 40

CLAIMS:

1. An electronic communication system (100), having
- at least one base station (10) having at least one antenna unit (16: 16a, 16b), in particular in coil form, which base station (10) is arranged in particular on or in an object to be secured against unauthorized use and/or against unauthorized access, such as on or in, say, a means of transport or on or in an access system, and
- at least one transponder station (40), in particular in data-carrier form, having at least one antenna unit (44: 44a, 44b), in particular in coil form, which transponder station (40)
-- may in particular be carried with him by an authorized user and/or
-- is designed to exchange data signals (22, 24) with the base station (10), in which case, by means of the data signals (22, 24)
--- the authorization for use and/or access can be determined and/or
--- the base station (10) can be controlled accordingly,

characterized in that
- there is arranged in the base station (10) at least one first delay element (17) for setting a defined, and in particular substantially constant, signal transit time (t_1) within the base station (10) and/or
- there is arranged in the transponder station (40) at least one second delay element (47) for setting a defined, and in particular substantially constant, signal transit time (t_2) within the transponder station (40).

2. A communication system as claimed in claim 1, characterized in that the first delay element (17) and/or the second delay element (47) are/is arranged to be settable (e), multistage (a, b, ... y, z) and switchable (s) and have/has
- at least one digital gate subject to a known signal transit time and/or
- at least one filter and/or
- at least one clocked shift register.

3. A communication system as claimed in claim 1 or 2, characterized in that

- there is connected downstream of the last stage (17z) of the first delay element (17) at least one first decision-making unit (18) that is connected to at least one control unit (12) of the base station (10) and/or to at least one receiver unit (19b) of the base station (10), and/or
- there is connected downstream of the last stage (47z) of the second delay element (47) at least one second decision-making unit (48) that is connected to at least one control unit (42) of the transponder station (40) and/or to at least one receiver unit (49a) of the transponder station (40).

4. A base station (10) for an electronic communication system (100) as claimed in any one of claims 1 to 3, characterized by

- at least one receiver unit (19b) for receiving the data signals (24) from the transponder station (40), which receiver unit (19b) is connected to the antenna unit (16b) associated with the base station (10),
- at least one control unit (12), in particular a microcontroller unit, for controlling the base station (10), which control unit (12) is connected to the receiver unit (19b) and is preferably connected upstream of the first delay element (17),
- the at least one first delay element (17) for setting the defined, and in particular substantially constant, signal transit time (t_1) within the base station (10), and
- at least one transmitter unit (19a) for transmitting the data signals (22) to the transponder station (40), which transmitter unit (19a) is connected to the antenna unit (16a) associated with the base station (10) and is preferably connected downstream of the first delay element (17).

5. A transponder station (40) for an electronic communication system (100) as claimed in any one of claims 1 to 3, characterized by

- at least one receiver unit (49a) for receiving the data signals (22) from the base station (10), which receiver unit (49a) is connected to the antenna unit (44a) associated with the transponder station (10) and is preferably connected upstream of the second delay element (47),
- the at least one second delay element (47) for setting the defined, and in particular substantially constant, signal transit time (t_2) within the transponder station (40),

- at least one control unit (42), in particular a microcontroller unit, for controlling the transponder station (40), which control unit (42) is preferably connected downstream of the second delay element (47), and
- at least one transmitter unit (49b) for transmitting the data signals (24) to the base station (10), which transmitter unit (49b) is connected to the antenna unit (44b) associated with the transponder station (40) and is preferably connected downstream of the control unit (42).

6. A transponder station as claimed in claim 5, characterized in that the transponder station (40) is arranged in at least one data carrier, and in particular in at least one card, and specifically in at least one chip card.

7. A method of detecting and/or guarding against at least one, in particular external, attack, and preferably at least one relay attack, on at least one electronic communication system (100) as defined in the preamble to claim 1, characterized in that there are/is set
- within the base station (10), a defined, and in particular substantially constant, signal transit time (t_1) and/or
- within the transponder station (40), a defined, and in particular substantially constant, signal transit time (t_2),

thus enabling the attack to be detected if the sum of
- the signal transit time (t_1) within the base station (10),
- the signal transit time (t_2) within the transponder station (40) and
- twice the signal transit time (t_s) of the data signals (22, 24) between the base station (10) and the transponder station (40)

exceeds a defined threshold value ($t_{s,max}$).

8. A method as claimed in claim 7, characterized in that

[a.1] a pulse that forms at least part of the data signal (22) to be transmitted to the transponder station (40) is conveyed within the base station (10) to at least one first delay element (17),

[a.2] the pulse, having been delayed by the first delay element (17), is then fed to at least one transmitter unit (16a) associated with the base station (10) and is received directly,

i.e. with no relevant additional delay, by at least one receiver unit (16b) associated with the base station (10),

[b] the pulse that forms at least part of the data signal (22) to be transmitted to the transponder station (40) is fed through the entire first delay element (17a, 17b ... 17y, 17z) substantially at the same time,

[c] at least one first decision-making unit (18) that is connected downstream of the last stage (17z) of the first delay element (17) signals to at least one control unit (12) of the base station (10) whether it is the delayed pulse (see method step [a.2]) or the pulse fed through the entire first delay element (17a, 17b, ... 17y, 17z) (see method step [b]) that arrives at the first decision-making unit (18) first, and

[d] the first delay element (17) is so set or switched or corrected that the delayed pulse (see method step [a.2]) and the pulse fed through the entire first delay element (17a, 17b, ... 17y, 17z) (see method step [b]) arrive as nearly simultaneously as possible.

9. A method as claimed in claim 7 or 8, characterized in that

[e] a pulse that forms at least part of the data signal (22) received from the base station (10) is conveyed within the transponder station (40) to at least one second delay element (47),

[f] the pulse that forms at least part of the data signal (22) received from the base station (10) is also fed through the entire second delay element (47a, 47b ... 47y, 47z) substantially at the same time,

[c] at least one second decision-making unit (48) that is connected downstream of the last stage (47z) of the second delay element (47) signals to at least one control unit (42) of the transponder station (40) whether it is the delayed pulse (see method step [e]) or the pulse fed through the entire second delay element (47a, 47b, ... 47y, 47z) (see method step [f]) that arrives at the second decision-making unit (48) first, and

[d] the second delay element (47) is so set or switched or corrected that the delayed pulse (see method step [e]) and the pulse fed through the entire second delay element (47a, 47b, ... 47y, 47z) (see method step [f]) arrive as nearly simultaneously as possible.

10. Use of at least one electronic communication system (100) as claimed in any one of claims 1 to 3, and in particular of at least one transponder station (40) as claimed in claim 5 or 6, for authenticating and/or for identifying and/or for checking the authority to use,

enter or the like an object to be secured by means of the communication system (100), such as, say, a means of transport or an access system.

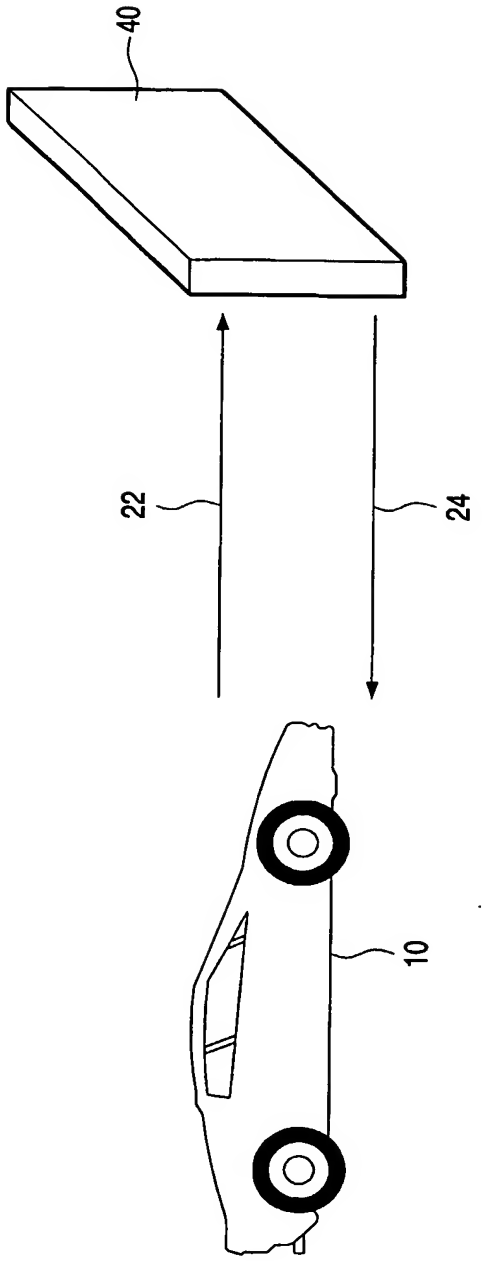


Fig.1A

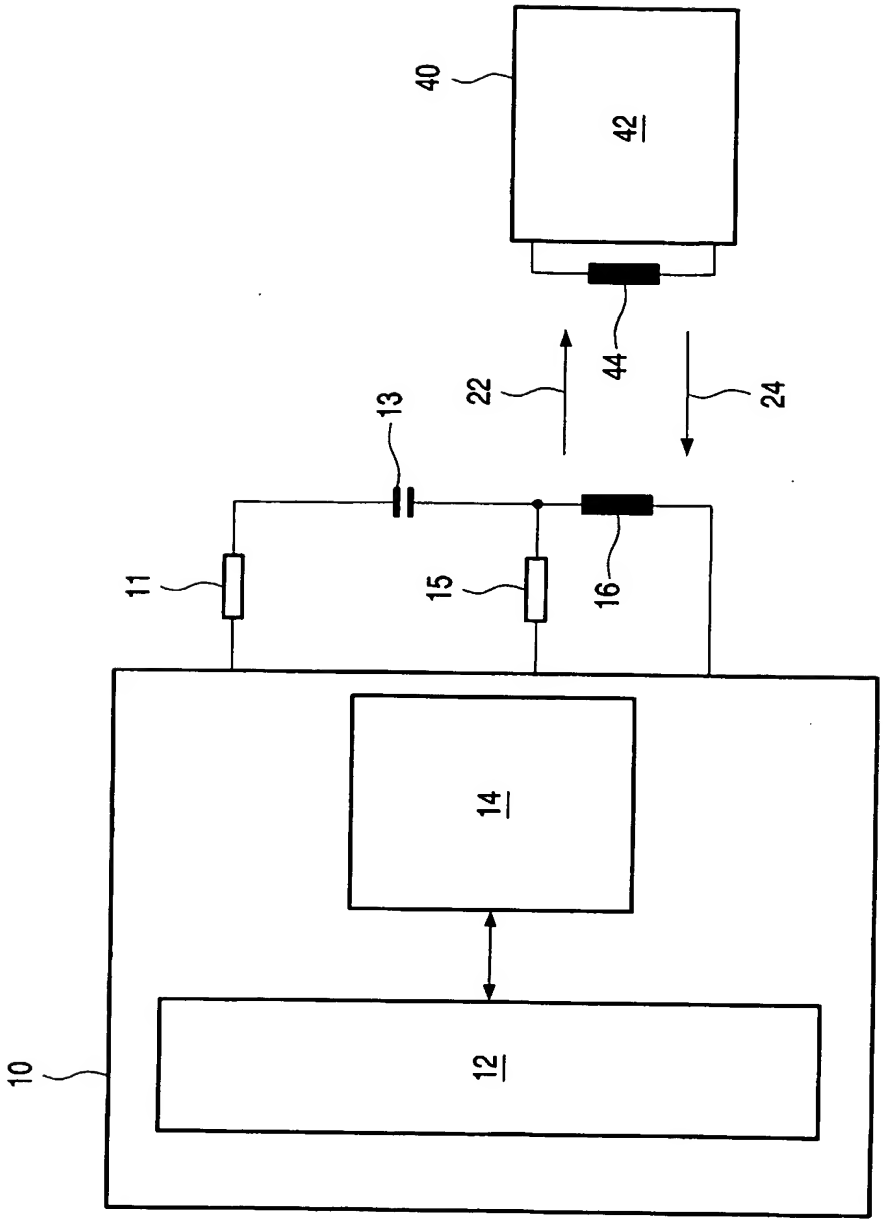


Fig.1B

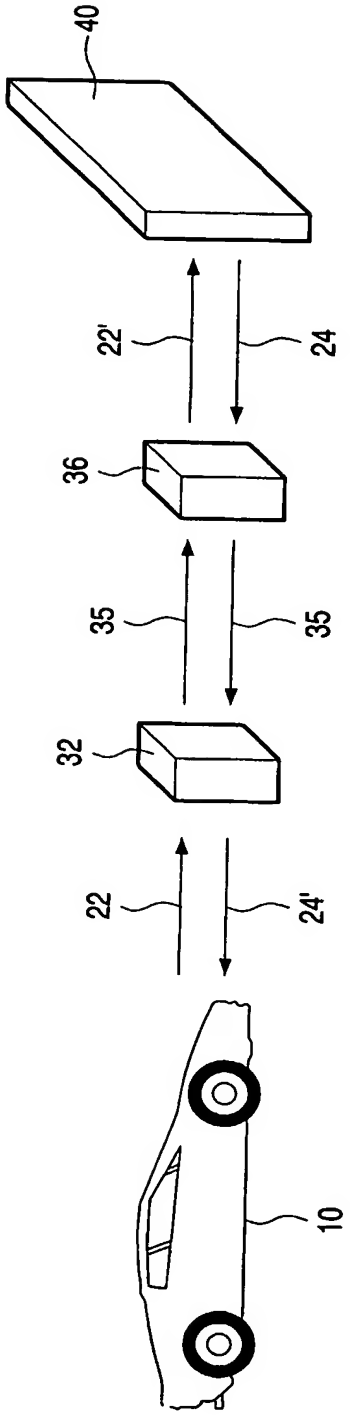


Fig.2A

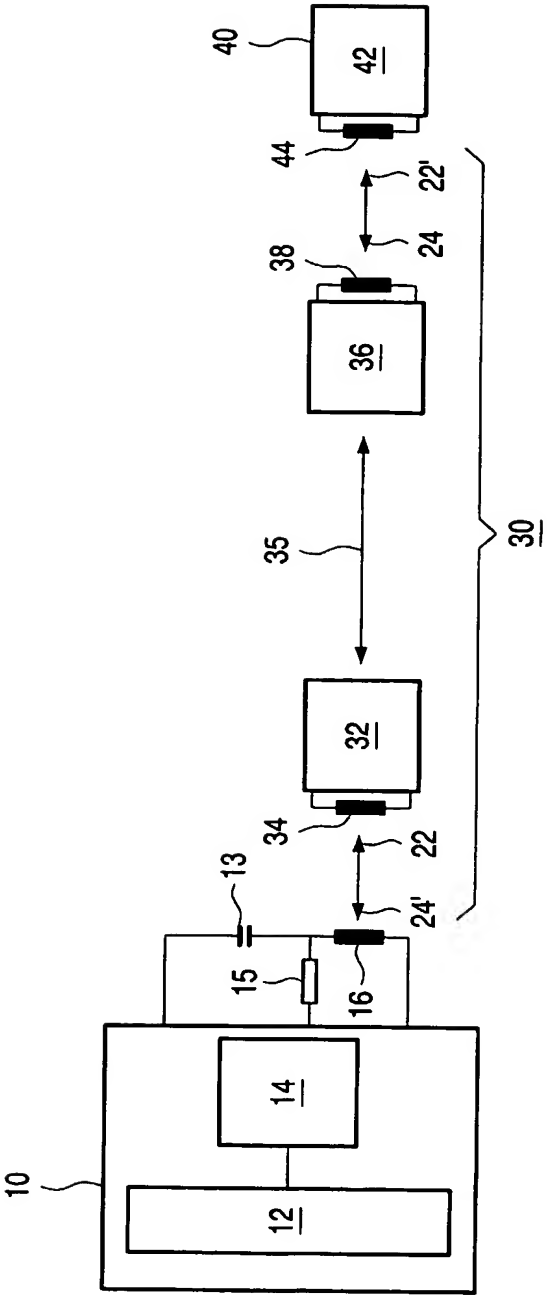


Fig.2B

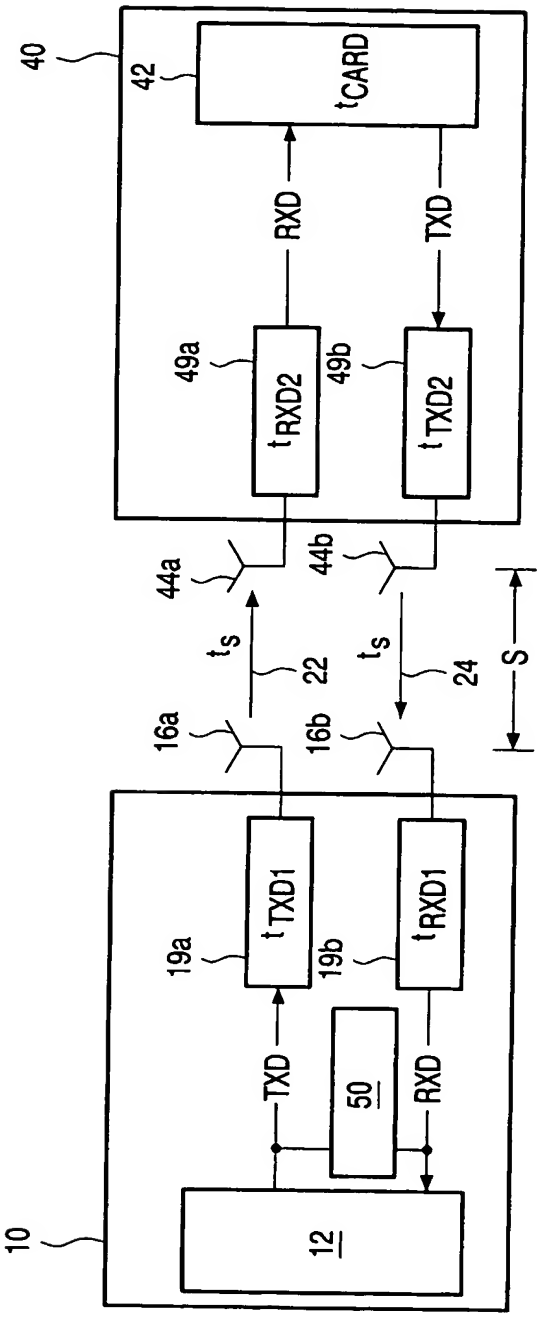

40
42
t_{CARD}
RXD
TXD
49a
t_{RXD2}
49b
t_{TXD2}
44a
44b
t_s
22
t_s
24
S
16a
16b
19a
t_{TXD1}
19b
t_{RXD1}
TXD
50
RXD
10
12

Fig.3

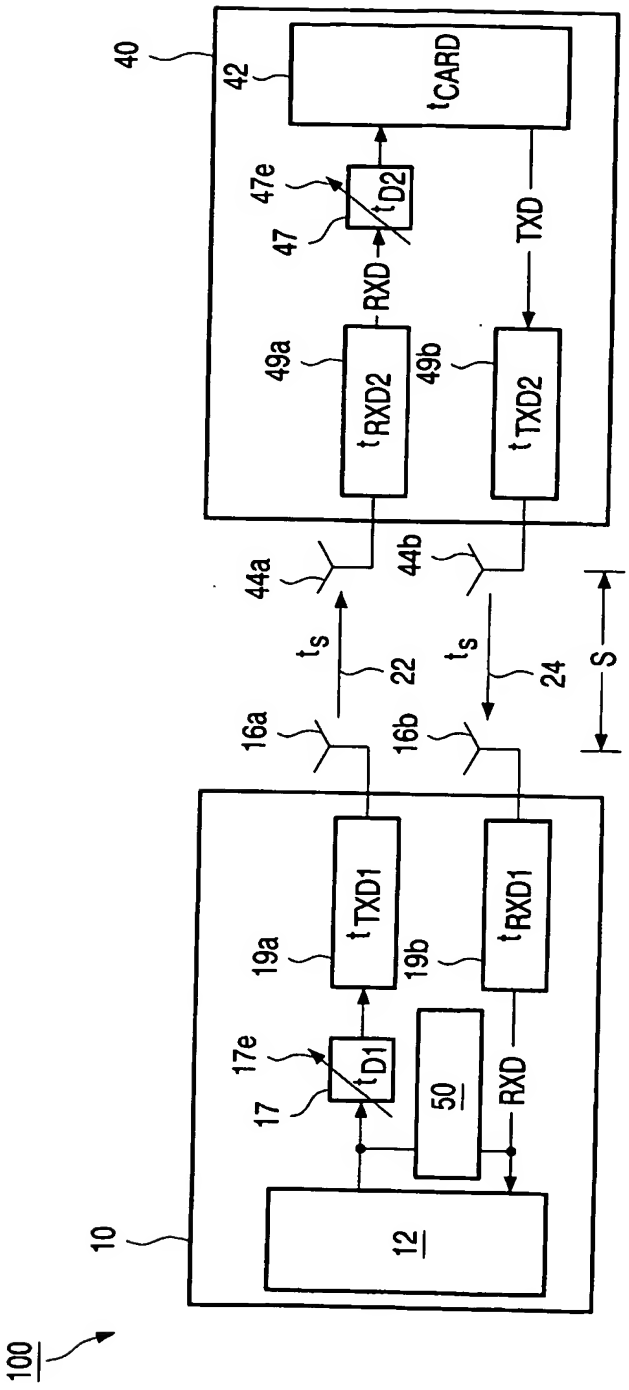

100
10
12
50
RXD
17
17e
t_{D1}
19a
19b
t_{TXD1}
t_{RXD1}
16a
16b
t_s
22
t_s
24
S
44a
44b
49a
49b
t_{RXD2}
t_{TXD2}
RXD
47
47e
t_{D2}
TXD
42
t_{CARD}
40

Fig.4

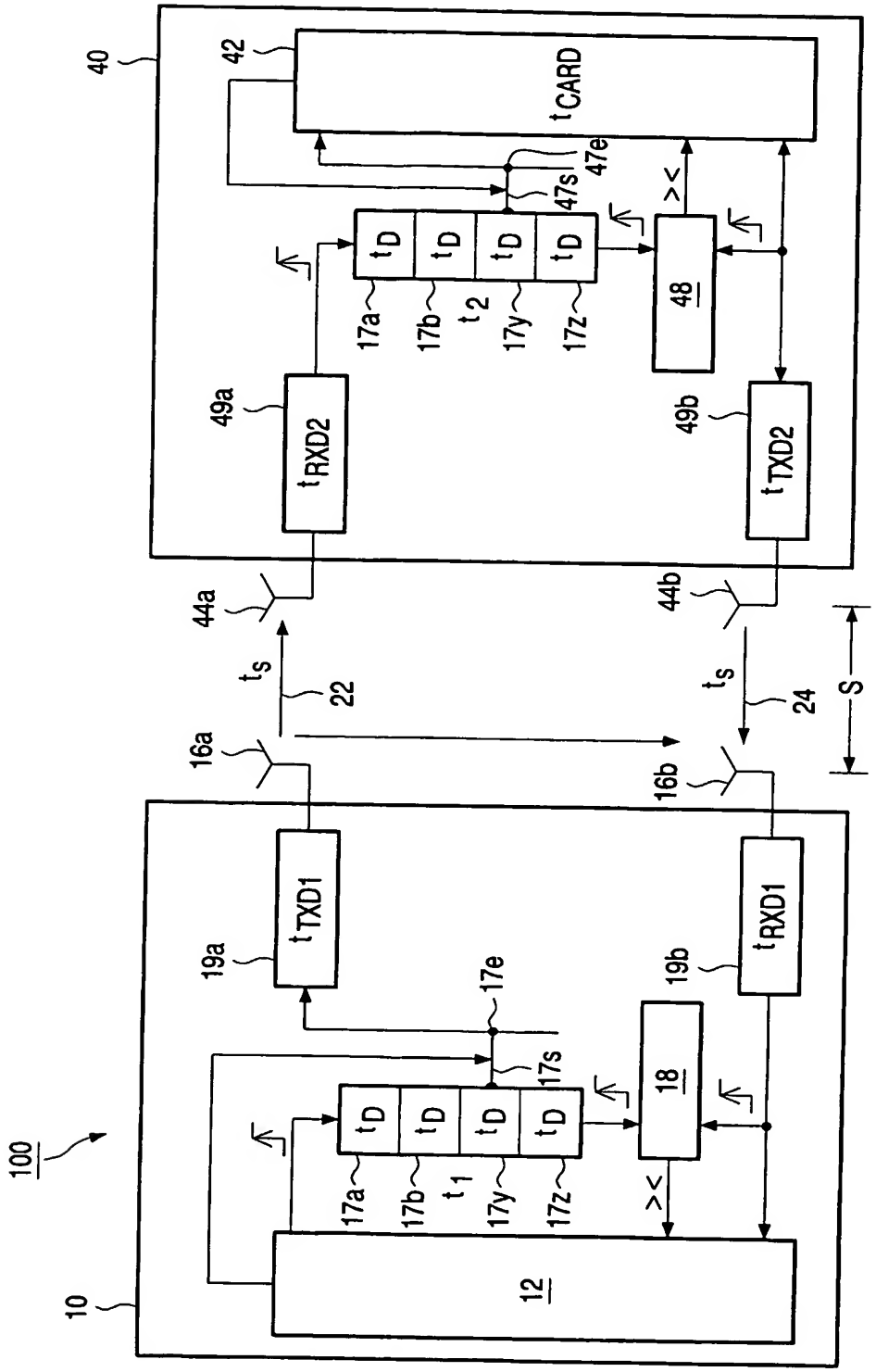

40
42
t_{CARD}
47e
47s
t_D
t_D
t_D
t_D
17a
17b
t_2
17y
17z
48
49a
t_{RXD2}
49b
t_{TXD2}
44a
44b
t_s
22
t_s
24
S
16a
16b
100
t_{TXD1}
19a
17e
17s
t_D
t_D
t_D
t_D
17a
17b
t_1
17y
17z
18
19b
t_{RXD1}
12
10

Fig.5

INTERNATIONAL SEARCH REPORT

Internat ılication No
PCT/IB 03/05378

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 B60R25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 983 916 A (MARQUARDT GMBH) 8 March 2000 (2000-03-08) abstract paragraph '0005! - paragraph '0013! paragraph '0030! - paragraph '0031!	1-10
A	EP 1 004 726 A (MANNESMANN VDO AG) 31 May 2000 (2000-05-31) abstract paragraph '0004! - paragraph '0008!	1-10
A	US 6 353 776 B1 (ROEHRL THOMAS ET AL) 5 March 2002 (2002-03-05) abstract column 1, line 55 - column 3, line 22	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2004	23/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Teutloff, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internati lication No
PCT/IB 03/05378

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0983916 A	08-03-2000	DE 19941428 A1	15-06-2000
		EP 0983916 A1	08-03-2000
EP 1004726 A	31-05-2000	DE 19854128 A1	31-05-2000
		EP 1004726 A2	31-05-2000
		KR 2000047709 A	25-07-2000
US 6353776 B1	05-03-2002	EP 1069265 A2	17-01-2001